CRYPTOGRAPHY AND CERTIFICATE AUTHORITIES IN GAMING MACHINES

This document is based on and claims the priority benefit of copending provisional application serial 60/161,591.

BACKGROUND OF THE INVENTION

1. Field of the Invention.

The present invention relates to an apparatus and method for encrypting communications on a network bus in a gaming system, and more particularly, to an apparatus and method where a certificate authority server manages keys used to secure communications on a network bus in a gaming system.

2. Statement of the Problem.

Conventional gaming machines include a processor, a rules library, a random number generator and an interactive display. In the casino, these conventional gaming devices are, typically, stand-alone type machines. Increasingly, the gaming machines in a casino are networked via a network bus to a gaming server. This networking is desired because it allows the casino to monitor wagering and other activities performed at each of the networked gaming machines. Since the monitoring of wagering and other activities performed at each of the networked gaming machines can include financial information, the casino desires that the communications over the network bus be secure.

In considering secure gaming communications, there are several important goals that should be addressed. The network bus should ensure privacy. Privacy, also termed confidentiality, is the condition where the information is kept secret from all but those

authorized to access the information. In the gaming environment, privacy can apply to the transmitted information as well as the identity of a player of the gaming machines.

In addition, information transmitted over the network bus should be authenticated. Authentication ensures that the content, integrity of the transmitted information, origin of the transmitted information, date of transmission, time of transmission and other attributes of the transmitted information have not been tampered with during transmission.

Additionally, entities transmitting information over the network bus should not be capable of repudiating the transmission. Cryptographic services that facilitate non-repudiation prevent a player and/or a casino from denying a previous action or commitment. The casino desires non-repudiation, especially, to enforce payment by a player that has wagered and lost. Conversely, the player desires non-repudiation to enforce payment by the casino when the player wins.

As a result of networking of the gaming machines, the ubiquity of the Internet, greater connectivity between networks, and the support for electronic commerce both inside and outside the casino, the casino desires secure communications over the network bus that provides privacy, authentication and non-repudiation. Therefore, a need exists to provide these services to support secure communication over the network bus between the gaming server and the gaming machines in a casino.

In addition, the casino may decide or desire to connect the gaming server and, hence, the network bus and all networked gaming machines, to an outside network. Networking the casino to an outside network may be advantageous for a gaming entity that owns several casinos in different locations. For example, the connection of each casino to a centralized computer would provide centralized accounting of financial information for all the casinos operated by the gaming entity.

If casinos are connected to outside networks, however, it is critical that communications originating within the casino (including gaming machines and the gaming server) remain secured against misuse or tampering by an unauthorized party after the information exits the physical protection of the casino. This desire for secured communications becomes particularly important when financial information is transmitted by the casino over the outside network. Consequently, a need exists for a secure communication link between the gaming server in a casino and an outside network.

In addition, the connection between gaming machines requires various transmission and/or data protocols. These protocols are typically created as standards in the industry. However, a game manufacturer would like to control the connection between the gaming machines such that only authorized personnel can connect the gaming machines. Therefore, a need exists for a technique to control the connection between the gaming machines such that only authorized personnel can properly connect the gaming machines.

Additionally, some casino players may prefer playing a specific gaming machine. However, the player may be in a remote location and unable to travel to the casino to play. In such instances, the casino can connect a gaming machine to an outside network so that the player can connect to the outside network via a remote computer and play, even though absent from the casino. In such instances, a need exits for a secure network that provides privacy, authentication and non-repudiation so that the player can play and both the player and casino can be confident in the knowledge that the transmitted information is secure and that the rules of the game will be upheld with integrity.

3. <u>Solution to the Problem</u>.

The present invention provides a method and apparatus that allows secure communication in a casino between networked gaming

machines and a gaming server. With the present invention, privacy is ensured; communication is authenticated; and messages cannot be repudiated.

Additionally, the present invention discloses a method and apparatus that provides secure communications between the casino and an outside network. The present invention is especially advantageous if the gaming entity manages machines at multiple casinos in different locations and the gaming entity requires quick, yet secure retrieval of information over the outside network.

In addition, the present invention provides a method and apparatus for secure communications between each gaming machine. In this regard, this secure communication allows for the connection between the gaming machines to be controlled by the game manufacturer such that the gaming machines cannot be connected unless the cryptographic technique used to secure the communications between the gaming machines is known.

Lastly, the present invention provides secure communications between the casino and a remote player over an external network. The present invention is especially critical in ensuring that transmitted information between player and casino is kept confidential and indecipherable by unauthorized individuals intercepting the transmitted information.

SUMMARY OF THE INVENTION

The present invention provides a casino gaming system having a plurality of gaming machines. In the Asymmetric case, a gaming server is provided that includes a plurality of long term keys from which it may generate keys used to communicate between gaming machines and also between the gaming machines and server. Prior to use, each of the keys is time stamped. The gaming server also includes a random number generator that is used to facilitate generation of the keys. The gaming server also includes an encryption algorithm.

A network bus is provided that interconnects the gaming machines and the gaming server. The network bus provides a communication link for transmitting information between the gaming machines and the gaming server. The gaming server uses the encryption algorithm to encrypt the keys and transmits the encrypted keys over the network bus to the gaming machine. Likewise, the gaming machines use the keys to encrypt information and transmit the encrypted information over the network bus. In one aspect, the encrypted information is transmitted via the network bus to another of the gaming machines. In another aspect, the encrypted information is transmitted via the network bus to the gaming server.

In another embodiment, the casino gaming system includes an outside network that is connected to the gaming server. A remote computer is also provided that connects to the outside network so that the encrypted information is transmitted over the network bus and the outside network to the remote computer. In one aspect, the outside network comprises the Internet.

In another embodiment of the present invention, the gaming server is a certificate authority server having a memory. In this aspect, the keys are public keys of asymmetric key pairs which are

stored in the memory at the certificate authority server. In addition, the certificate authority server may generate and transmit the public keys over the network bus to the gaming machines, or the public/private key pairs may be generated by a third party and delivered to the certificate authority for authentication.

In a further embodiment of the present invention, a plurality of access switches are each connected to a different one of the gaming machines. The network bus is connected to the gaming server and each of the access switches. In this embodiment, an outside network is connected to the gaming server and the access switches provide a communication link between specific gaming machines and a remote computer over the outside network when the specific gaming machine is idle, so as to enable a remote player of the remote computer to play the specific gaming machine.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates one embodiment of the casino gaming system of the present invention;

Fig. 2. is a flow chart showing a method for communicating information using a casino gaming system of the present invention;

Fig. 3 illustrates an embodiment of the casino gaming system of the present invention using a certificate authority server;

Fig. 4 illustrates another embodiment of the casino gaming system of the present invention; and

Fig. 5 is another embodiment of a method for communicating using the casino gaming system of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

I. Overview

In Fig. 1, a highly simplified gaming system 100 includes a gaming server 110 that is connected to a plurality of gaming machines 120-124 via network bus 130. The gaming server 110 can comprise, for example, a micro-computer or a network server. The connection of the gaming server 110 to network bus 130 can comprise, for example, a hard-wired communication link connection or a wireless communication link connection. The network bus 130 also connects to the plurality of gaming machines 120-124 that are located in a casino. In one embodiment, the gaming machines 120-124 can comprise conventional stand-alone gaming machines that are networked to the gaming server 110 via the network bus 130. The gaming machines 120-124 can also allow play of various conventional casino games such as, but not limited to, slots, poker, blackjack, etc.

In one embodiment, the casino gaming system 100 can also includes an outside network 140, such as, for example, the Internet, a Local Access Network (LAN) or a Wide Area Network (WAN). At least one remote computer 150 is connected to the outside network 140. In one embodiment, the connection of the remote computer 150 to the outside network 140 also enables the remote computer 150 to connect to the gaming server 110, and hence, the network bus 130 and the gaming machines 120-124. In this embodiment, a remote player of the remote computer 150 can play a specific one of the gaming machines 120-124 on the network bus 130 through the connection to the outside network 140. As such, a remote player can play a specific one of the gaming machines 120-124 via an outside network 140 without having to be physically in the casino.

The connection between the network bus 130 and the gaming server 110 is conventionally known in the art, and the connection can

include other equipment (not shown) such as, for example a router. The connection between the gaming server 110 and the outside network 140 is also know in the art, and the connection can include various security features, such as, for example, a firewall. The connection between the remote computer 150 and the outside network 140 can include, for example, a hardwire connection, a wireless connection or a modem connection. It should be appreciated that the present invention is not limited to the manner in which the components are connected, since such connection of the components is known in the art.

In the gaming system 100 of the present invention, information that is transmitted over the network bus 130 and the outside network 140 must be secure, especially with regard to financial information, such as, for example, player credit card information, player wagering information and casino pay-out information. To ensure a secure transmission of information over the network bus 130 and the outside network 140, the information is encrypted using various cryptography techniques. Key cryptography and certificate authority techniques are described below with regard to secure encrypted information transmission in a casino gaming system 100.

II. Key Cryptography

A. Casino Gaming System using Keys

In Fig. 1, the casino gaming system 100 includes a network 130 that interconnects gaming machines 120-124 and gaming server 110. The network bus 130 provides a communication link for transmitting information between the gaming machines 120-124, themselves, and between the gaming machines 120-124 and the gaming server 110. It should be noted that the computational capabilities of the gaming server 110 should generally exceed those of the gaming machines 120-124, at least with respect to cryptographic operations. In this regard, many computer systems

have architecture and/or use compilers that physically limit the bit length of an integer, such as, for example, 32 bit length. However, key cryptography requires the use of very large integers having a bit length such as, for example, 64 or 256 bits. To enable these computer systems to arithmetically manipulate these integers, cryptographic primitives are required. Cryptographic primitives include algorithms that process large integers during various arithmetic processes. It should also be noted that these cryptographic primitives can be any algorithm that allows processing of large bit length integers by these bit-limited computer systems.

However, these primitives should be able to support Rivest, Shamir, and Adleman (RSA), El Gamal and other known key cryptographic algorithms. It should also be appreciated that the present invention is not limited by the algorithms and/or cryptography used to manipulate these large bit length integers, and the present invention encompasses any technique known and practiced in the art.

The gaming server 110 also includes keys 160. For example, the keys 160 can comprise, as will be described later, symmetric keys, asymmetric keys or session keys. The keys 160 include a time stamp 165 that indicates a period of time for which each of the keys 160 is valid. The time stamp 165 also ensures that the keys 160 are changed on a periodic basis to provide a more secure communication link.

The gaming server 110 also includes a random number generator 170 that is used by the gaming server 110 to generate the keys 160. The random number generator 170 can comprise a pseudo-random number generator and/or a random number generator that has been approved by a governmental regulation agency. The generation of the keys 160 by using the random number generator 170 is known in the art and the present invention should not be limited to any one technique for generating the keys 160. It should also be appreciated that in another embodiment the

random number generator 170 is optional. In this embodiment, the gaming server 110 receives the keys 160 from another device (not shown) connected to the network bus 130.

It should also be appreciated that the gaming server 110 can also include an encryption algorithm 180. The gaming server 110 uses the encryption algorithm 180 to encrypt information or data before it is transmitted over the network bus 130. The encrypted information is decrypted before it is used. The encryption algorithm 180 can comprise, for example, a symmetric key or one of an asymmetric key pair as will be explained herein below.

In one embodiment, the gaming server 110 transmits at least one of the keys 160 over the network bus 130 to a gaming machine 120. It should be appreciated that the gaming server 110 can transmit one of the keys 160 to any one of the gaming machines 120-124 on the network bus 130. However, for ease of description, this discussion will focus on transmission to gaming machine 120.

In this embodiment, the gaming machine 120 uses the keys 160 to encrypt information, such as, player credit card information, player identification information, wagering information and casino payout information. This encrypted information is transmitted over the network bus 130.

In one aspect, the encrypted information is transmitted over the network bus 130 to the gaming server 110. In another aspect, the encrypted information is transmitted over the network bus 130 from gaming machine 120 to another of the gaming machines 122-124. At the other gaming machine 122-124, the encrypted information is decrypted based on the type of key 160 used as will be described herein below.

In another embodiment, the casino gaming system 100 includes an outside network 140 that is connected to the gaming server 110. The outside network 140 is connected to a remote computer 150. The outside network 140 comprises, for example, the

Internet, a local access network (LAN) or a wide area network (WAN). In this embodiment, the gaming server 110 includes various known security mechanisms (not shown), such as, a firewall.

In this embodiment, the gaming server 110 transmits the key 160 to gaming machine 120. The gaming machine 120 encrypts information using the key 160 and transmits the encrypted information over the network bus 130. In one aspect of the present invention, the encrypted information is transmitted to the gaming server 110. In another aspect of the present invention, the encrypted information is transmitted by the gaming machine 120 to another of the gaming machines 122-124 on the network bus 130. In even another aspect, the encrypted information is transmitted to the outside network 140 and, ultimately, to the remote computer 150. Once the encrypted information has been received, it is decrypted based on the type of key 160 used, as will be described herein below. The information is then processed as required.

1. Symmetric Keys

As explained above, the keys 160, in one embodiment, comprise symmetric keys. Symmetric keys, also termed private keys, use a unique key to encrypt and exchange information between two parties. In this embodiment, gaming machine 120 (the sender) and gaming server 110 (the recipient) share a symmetric key k which is secret. In this embodiment, the gaming machine 120 encrypts information m before transmitting it over the network bus 130 to the gaming server 110. If symmetric encryption algorithm E and symmetric key k are used, the encryption of m by E under k is denoted $c = E_k(m)$ where c represents the cipher-text associated with information m. Therefore, gaming machine 120 transmits cipher-text c over the network bus 130 to the gaming server 110. At the gaming server 110, the cipher-text c is decrypted using the symmetric key

k. The gaming server 110 applies the decryption algorithm $m = E_k^{-1}(c)$ to decrypt cipher-text c and obtain information m.

In addition, the symmetric key k can also be a session key . A session key is used for a specific exchange of a message m between two parties, such as, two gaming machines 120 and 122 or between a gaming machine 120 and the gaming server 110. In this embodiment, gaming machine 120 desires to communicate with gaming machine 122. The gaming server 110 contains a symmetric encryption function , E, that allows the encryption of a *session key*, k, that will be sent by the gaming server 110 in an encrypted format to gaming machines 120 and 122. In this embodiment, $E_{k_i}(m)$ represents the encryption of message m under encryption algorithm E using key k_i, and $E_{k_i}^{-1}(m)$ represents the decryption of message m under encryption algorithm E using key k_i. In order to allow the communication between gaming machines 120 and 122, the gaming server 110 generates a new unique session key k, and the gaming server 110 sends $E_{k_1}(k)$ to gaming machine 120 and $E_{k_2}(k)$ to gaming machine 122. The gaming machines 120 and 122 each can recover the session key k by forming $k = E_{k_1}^{-1}(E_{k_2}(k)) = E_{k_{21}}^{-1}(E_{k_2}(k))$. Using the session key k, gaming machine 120 can communicate message m to gaming machine 122 by sending $E_k(m)$ to gaming machine 122, gaming machine 122 can form $m = E_k^{-1}(E_k(m))$ to recover the message. It should be appreciated that this technique can be used with communciations between any device connected to the network bus 130 and should not be limited to communications between only gaming machines 120 and 122. In addition, in one embodiment, the gaming server 130 generates the session key k using the long term asymmetric key 160 as a seed to random number generator 170. In another embodiment, the gaming server can use any one way function that is non-invertable to generate the session key k.

However, it should be appreciated that the present invention can use any technique known in the art to generate the session key k, and the present invention should not be limited to only those disclosed.It should be noted that the cipher-text c is described as being transmitted only from the gaming machine 120 to the gaming server 110. However, it should be understood that the cipher-text c can be transmitted from the casino gaming server 110 to the gaming machine 120 using the same symmetric key 160. Moreover, it should be appreciated that cipher-text c can be transmitted from any one of the gaming machines 120-124 to the gaming server 110 or vise versa using the symmetric key 160. In addition, the cipher-text c can be transmitted from the gaming machines 120-124 or the gaming server 110 to the outside network 140 and the remote computer 150 (or vise versa) using the symmetric key 160 as described above. It should further be appreciated that the encryption algorithm 180 used by the gaming server 110 to encrypt and transmit the keys 160 to the gaming machines 120-124 can comprise a symmetric key 160, and the key 160 can be encrypted and/or decrypted as described above with reference to information m. In a preferred embodiment, the symmetric key 160 uses the Data Encryption Standard (DES) or one of the variants of DES such as triple-DES, DES-X or Advanced Encryption Standard (AES).

2. Asymmetric Keys

As mentioned above, the keys 160 can comprise asymmetric keys. Asymmetric keys, also termed public keys, use two different keys in a transaction. The asymmetric key pair consists of a public and a private key. The public key is made available to all devices on the network bus 130 and the outside network 140 while the private key is kept secret. The essential feature of a public key cryptographic system is that knowledge of a public key does not provide computational information about the private key.

In this embodiment, the asymmetric key pair 160 is represented by (u,r) where u represents the public key and r represents the private key. The gaming machine 120 acquires the public key u of the gaming server 110 from the gaming server 110 or another device (not shown) connected to the network bus 130 or the outside network 140. The gaming machine 120 encrypts information m using public key algorithm E_u. As a result, the cipher-text c is $c = E_u(m)$. The cipher-text c is transmitted to the gaming server 110 over the network bus 130. The private key algorithm E_r^{-1} is used by the gaming server 110 to decrypt the cipher-text c and therefore obtain the information $m = E_r^{-1}(E_u(m))$. In this embodiment, it should be appreciated that each of the gaming machines 120-124, the gaming server 110 and the remote computer 150 have a unique asymmetric key pair (u,r). The public key u is provided to the sending party and only the private key r can decrypt information encrypted by the public key u. It should also be appreciated that the asymmetric key technique can be used by any device connected to the network bus 130 or the outside network 140 so long as the appropriate public key u is used to encrypt the information m and the cipher-text c is sent to the device having the corresponding private key r.

In addition, it should also be appreciated that the encryption algorithm 180 can comprise the public key u of the asymmetric key pair (u,r). The gaming server 110 encrypts the key 160 using the public key u and transmits the encrypted key 160 to the appropriate gaming machine 120-124 or remote computer 150 having the corresponding private key r. In a preferred embodiment of the present invention, the asymmetric keys 160 comprise Rivest, Shamir, and Adleman (RSA) and El Gamal asymmetric algorithms.

3. Digital Signatures

In another embodiment, the keys 160 can comprise a digital signature. A digital signature can be constructed by reversing the asymmetric key technique described above. In this embodiment, the gaming machine 120 uses the private key algorithm E_r^{-1} to encrypt the information m where the cipher-text is $c = E_r^{-1}(m)$. The cipher-text c is transmitted to the gaming server 110 where the cipher-text c is decrypted to obtain information m by applying the public key algorithm $m = E_u(E_r^{-1}(m))$. Since the private key algorithm E_r^{-1} is only known by the gaming machine 120, the gaming server 110 can be particularly certain that the information m was sent by the gaming machine 120 because only the public key algorithm E_u is able to decrypt cipher-text c that has been encrypted using the private key algorithm E_r^{-1}.

As shown above, the digital signature is a variation of the asymmetric key technique described above and can be fully implemented using asymmetric keys. The digital signature provides an extra security feature that allows the receiving party to verify the sending party. This technique is particularly useful in the casino gaming system 100 when financial information, such as, credit card information, is being transmitted over the network bus 130.

It should be appreciated that the digital signature has been disclosed with reference to the gaming machine 120 and the gaming server 110 but should not be limited as such. The digital signature can be used by all devices connected to the network bus 130 and/or the outside network 140. In addition, the encryption algorithm 180 used by the gaming server 110 to encrypt and transmit keys 160 over the network bus 130 can comprise a digital signature.

B. Method For Using Keys

As shown in Fig. 2, the present invention includes a method for communicating information using a casino gaming system 100 having gaming machines 120-124 and a gaming server 110. The method includes establishing a first communication link (network bus 130 in Fig. 1) between the gaming machines 120-124 and the gaming server 110 (step 210). A second communication link (outside network 140 in Fig. 1) is established between the gaming server 110 and the remote computer 150 (step 220). It should be appreciated that the outside network 140 can comprise the Internet, a local access network (LAN) or a wide area network (WAN).

The gaming server 110 includes keys 160. In one embodiment, the gaming server 110 includes a random number generator 170 that randomly generates the keys 160 (step 230). The gaming server 110 can also include an encryption algorithm 180 that is used to encrypt the keys 160 at the gaming server 110 (step 240). It should be appreciated that the keys 160 and the encryption algorithm 180 can comprise symmetric keys or asymmetric keys that function as described herein above.

The key 160 is transmitted from the gaming server 110 to, in one embodiment, a gaming machine 120 (step 250). It should be appreciated that the gaming server 110 can transmit the key 160 to any other device connected to the network bus 130 or the outside network 140. The key 160 is used by the gaming server 110 to encrypt information sent from the gaming machine 120 (step 260). The encrypted information is transmitted over the first communication link (network bus 130) and/or the second communication link (outside network 140) (step 270). It should be appreciated that the encrypted information can be transmitted to another of the gaming machine 122-124, the gaming server 110 or the remote computer 150. Once the encrypted information is received, it is decrypted by the receiving device (such as, for example, gaming server 110) using a technique

based on the type of key 160 used as described herein above (step 280).

It should be appreciated that the method described with reference to gaming machine 120 and gaming server 110 is only for ease of description and should not be interpreted as being limited as such. It should be appreciated that the above described method can be used by any device connected to the network bus 130 and/or the outside network 140.

III. Certificate Authority

In general, as shown in Fig. 3, a certificate authority server 300 guarantees the identity of a device connected to the network bus 130 or connected to the outside network 140. The certificate authority 300 guarantees the identity by granting a unique public key 315 to each of the devices (as shown in Fig. 3, such as, gaming machines 120-124, gaming servers 330-332 and certificate servers 340-342) connected to the network bus 130. The certificate authority server 300 can also grant a unique public key to certain devices (such as remote computer 150) that are connected to the outside network 140. As noted above, there can be other certificate authority servers 340 and 342 connected to the network 130. All the certificate authority servers 300, 340 and 342 can be connected in a hierarchical configuration which is known in the art. In addition, there may be gaming servers 330-332 that do not have the ability to guarantee the identity of a device connected to the network bus 130. However, these gaming server 330-332 have the ability to perform other operations on the network bus 130, as described above with reference to Fig. 1.

A. Casino Gaming System using a Certificate Authority

As shown in Fig. 3, another embodiment of the casino gaming system 100 includes a certificate authority server 300 that is used for communicating information using asymmetric key pairs including a

private key and a public key. In this embodiment, a network bus 130 interconnects the certificate authority 300 and the gaming machine 120-124. The network bus 130 can also be connected to other certificate authority servers 340-342 and gaming servers 330-332. The certificate authority server 300 includes a memory 310 that stores public keys 315. The public keys 315 can also include a time stamp (not shown) that indicates a time period that the asymmetric key pair is used. The certificate authority server 300 also includes a random number generator 320 that is capable of generating the asymmetric key pairs of the present invention.

The certificate authority server 300 is also connected to an outside network 140 and a remote computer 150 is connected to the outside network 140. The outside network 140 can comprise the Internet, a local access network (LAN) or a wide area network (WAN). In another embodiment, it should be appreciated that the outside network 140 can connect to a gaming server 330-332 or another certificate authority server 340-342. The certificate authority server 300 can include other security mechanisms (not shown) to facilitate connection to the outside network 140, such as, for example, a firewall. The remote computer 150 can connect to the outside network 140 via, a hard wired connection, a wireless connection or a modem connection.

For ease of discussion, the certificate authority server 300 will be described with regard to transmissions to and from gaming machine 120 and gaming server 330. However, it should be appreciated that the certificate authority server 300 can transmit to any device on the network bus 130 and/or the outside network 140, and these devices can communicate using the same techniques as previously described with regard to the gaming machine 120 and the gaming server 110 (in Fig. 1).

In the present embodiment, when the gaming machine 120 desires to communicate with the gaming server 330, the gaming

machine 120 requests a public key 315 from the certificate authority server 300. The certificate authority server 300 transmits a public key 315 to the gaming machine 120. The public key 315 is used by the gaming machine 120 to communicate with the gaming server 330 connected to the network bus 130. Prior to transmission of the pubic key 315, the certificate authority server 300 has verified the identity of the gaming server 330 and granted a unique asymmetric key pair to the gaming server 330. The verification is accomplished using various techniques known in the art. As a result of this verification, the certificate authority server 300 can guarantee the identity of the gaming server 330 and the validity of the public key 315 that is to be used by the gaming machine 120 to communicate with the gaming server 330.

In addition to transmitting the public key 315, the certificate authority server 300 signs the public key 315. The signing of the public key 315 uses an encryption algorithm that is similar to the symmetric and asymmetric keys, such as, a digital signature, as described above. Once the gaming machine 120 receives the signed public key 315, the public key 315 is validated using, as described above, symmetric or asymmetric key techniques. The gaming machine 120 uses the public key 315 to encrypt information and transmits that information over the network bus 130 to the gaming server 330.

As explained above, the gaming machine 120 can communicate with any other device connected to the network bus 130 and/or the outside network 140. However, these other devices must also be verified by the certificate authority server 300. As a result, the gaming machine 120 receives the appropriate public key 315 and transmits encrypted information to the appropriate device, such as, for example, other gaming machines 122-124, gaming severs 330-332, certificate authority servers 300, 340-342 and remote computer 150.

In a preferred embodiment, the certificate authority server 330 meets the X.509 (ISO/IEC 9594-8) standard.

IV. Remote Access

As shown in Fig. 4, another embodiment of the casino gaming system 100 includes switches 420, 422 and 424 that enable a remote player using a remote computer 150 to connect to and play a specific gaming machine 120-124 that is located in a casino.

A. Remote Access Casino Gaming System

In this embodiment, shown in Fig. 4, a network bus 130 interconnects a gaming server 110 and switches 420, 422 and 424. A certificate authority server 300 is also connected to the network bus 130. The certificate authority server 300 provides public keys 315 used for encrypting communications, as described above. The switches 420, 422 and 424 are connected to gaming machine 120, 122 and 124, respectively. In a preferred embodiment, the gaming machines 120, 122 and 124 are located in a casino. However, the physical location of the gaming machines 120, 122 and 124 should not be interpreted as limiting the present invention. The gaming server 110 is connected to an outside network 140 and a remote computer 150 is connected to the outside network 140.

In another embodiment, the outside network 140 can connect to the certificate authority server 300. The gaming server 110 can have various security features to facilitate connection to the outside network 140, such as, for example, a firewall. The outside network 140 can comprise the Internet, a local access network (LAN) or a wide area network (WAN). The remote computer 150 can be connected to the outside network 140 via a hard wired connection, a wireless connection or a modem connection.

The present invention allows a remote player using a remote computer 150 to connect to and play a specific gaming machine 120-

124 in a casino. For ease of description, the remote computer 150 will be described as connecting to gaming machine 120. However, it should be noted that the present invention encompasses the remote computer 150 connecting to any of the gaming machine 122-124 that are connected to the outside network 140. As such, the remote computer 150 connects to the outside network 140 which is connected to the gaming server 110. The remote computer 150 can be located in the casino, or the remote computer 150 can be located remotely from the casino, such as, but not limited to, a hotel connected to the casino.

To play the gaming machine 120, the remote computer 150 makes a request to the gaming server 110 to gain access to gaming machine 120. The request made by the remote computer 150 can include entering identification information that uniquely identifies the remote player of the remote computer 150. The identification information can comprise a password, credit card information, etc.

The gaming server 110 compares the identification information with a database. The database can include a listing of all passwords, a credit check of the credit card information or casino-specific credit information. If the identification information matches one of the entries in the database, the remote computer 150 is given access to the gaming machine 120 through switch 420.

It should be appreciated that, in another embodiment, the switch 420 disconnects the gaming machine 120 from access by the remote computer 150 when the gaming machine 120 is being used in the casino. The disconnection of the gaming machine 120 can be initiated by a casino player in the casino. In this embodiment, if a casino player in the casino does not want a remote player connecting to the gaming machine 120, the casino player can activate switch 420 to prevent a remote player from accessing the gaming machine 120.

In addition, governmental regulation may require that only one person at a time can play a gaming machine 120 in the casino. In this

case, the remote computer 150 receives a gaming machine unavailable signal when the gaming machine 120 is occupied and/or not idle, and the remote computer 150 is asked to choose another gaming machine 122-124. Conversely, if a remote computer 150 is accessing the gaming machine 120, a casino player cannot play the accessed gaming machine 120. In the casino, this disconnection is indicated by a light (not shown) or other indicators that verify that the gaming machine 120 is unavailable.

Once the remote computer 150 gains access to the gaming machine 120, the remote player can play the gaming machine 120. In one embodiment during play of the gaming machine 120, the remote player views a digital representation of the game being played on the gaming machine 120. The remote player can view and interact with the gaming machine 120 via other mechanisms that are known in the art.

The present invention should not be interpreted as being limited to the manner in which the remote player views and interacts with the play of the gaming machine 120. Furthermore, if the gaming machine 120 breaks down or malfunctions during play, the gaming machine 120 sends a signal to the remote computer 150 indicating that the gaming machine 120 is no longer available and the remote player is asked to play another game and is credited any winnings from the gaming machine 120.

In addition, the communication between the remote computer 150 and the gaming machine 120 can be encrypted using symmetric or asymmetric keys as described herein above. The gaming server 110 or the gaming machine 120 can document information with regard to the wagering during remote play of the gaming machine 120. Such information can include identification information about the remote player, amounts wagered, the time the remote player plays the gaming machine 120 and the location from which the remote player is playing the gaming machine 120.

B. Method Remotely Accessing Casino Gaming System

As shown in Fig. 5, a method is provided that allows a remote player to access and play a specific gaming machine 120-124 from a remote location. In this method, a request is received from an outside network 140 to access and play a gaming machine 120-124 (step 510). The request from the outside network 140 may be initiated by the input of identification information. The identification information can comprise a password, credit card information, etc. The gaming server 110 compares the identification information with a database.

The database can comprise a listing of all passwords, a credit check of the credit card information or casino-specific credit information. If the identification information matches one of the entries in the database, the remote computer 150 is given access to the gaming machine 120 through switch 420. It should be appreciated that, in another embodiment, the switch 420 disconnects the gaming machine 120 from access by the remote computer 150 when the gaming machine 120 is being played in the casino. It should further be appreciated that the present invention is not limited to the type of request that is made by the remote computer 150 for access to the gaming machine 120.

Based on the request, a secured communication link is provided between the outside network 140 and the gaming machine 120-124 (step 530). In one embodiment, the secured communication link is only provided if the gaming machine 120-124 is idle and/or not being played by another player (step 520). In this embodiment, if the gaming machine 120 is not idle, a gaming machine unavailable message is provided to the outside network 140 (step 540). Additionally, the remote player can be asked to choose another of the gaming machines 122-124.

Once the outside network 140 accesses a gaming machine 120-124, information can be documented (step 550). The information can include identification information about the remote player,

amounts wagered, the time the remote player plays the gaming machine 120 and the location from which the remote player is playing the gaming machine 120. When the remote player begins to play, the player views a digital representation of the gaming machine 120.

The foregoing discussion of the invention and as presented in Exhibit A (incorporated herein by reference) has been presented for purposes of illustration and description. Further, the description is not intended to limit the invention to the form disclosed herein. Consequently, variation and modification commensurate with the above teachings, within the skill and knowledge of the relevant art, are within the scope of the present invention.

The embodiment described herein and above is further intended to explain the best mode presently known of practicing the invention and to enable others skilled in the art to utilize the invention as such, or in other embodiments, and with the various modifications required by their particular application or uses of the invention. It is intended that the appended claims be construed to include alternate embodiments to the extent permitted by the prior art.

Cryptographic Services for Gaming

Rolf Carlson
Spring Creek Technologies, Corp.

Abstract

Increasingly, information security technologies will be applied to gaming. It will be necessary to have a certificate authority mechanism in order to support the information security services required for a trusted relationship between the player, house, and game owner. This document describes information services along with the key management mechanisms that will be required for the support of information security services in a gaming environment.

Introduction

In order to achieve a framework that satisfies the information security goals associated with modern gaming and electronic commerce, there needs to be an infrastructure that can maintain a collection of keys. Modern cryptographic functions rely upon keys to protect and unprotect information. More generally, cryptographic protocols and primitives use these keys to achieve each of the information security objectives. Because of the way digital information can be replicated without owner consent, the keys should be regarded as the secret. If this is the case, we now have a new problem of where and how to store the keys so that the information the keys protect is not compromised.

Until about 1974, the primary means for encrypting information to protect privacy used symmetric key techniques. Soon after, however, it was observed that public-key methods could solve the key update problem between two users that know each other. Getting two strangers to have confidence in the identity of each other and content of a transaction, however, was soon seen to be a problem. Digital signature and certificate authorities often rely upon public key

cryptography and were developed to solve some of the problems that untrusting parties face when engaging in digital commerce. In the next several sections we discuss information security goals, symmetric and asymmetric cryptography, and finally the application of certificate authorities to the gaming environment.

Information Security Goals

There are three goals of information security that are facilitated by cryptography: privacy, authentication, and non-repudiation. Providing a collection of services that satisfy these goals has been generally regarded as a necessary condition for a successful digital framework for electronic commerce. We make the same assumption about electronic gaming.

Privacy

Confidentiality or privacy is the condition where information is kept secret from all but those authorized to know the information. Encryption techniques will be used to ensure confidentiality. It should be noted that encryption does not necessarily provide authentication. Privacy can apply to individuals as well as information. Anonymous WWW surfing is an example of a problem requiring identity confidentiality. Game players may require that their identity not be divulged as a precondition for play. Confidentiality provides this service.

Authentication

Ensuring the identity of communicating parties to one another is called user authentication. Ensuring the content, integrity, origin, date of origin, time sent and other attributes of a message is called message authentication. Combining hashing techniques with other cryptographic primitives to form more complicated structures, called protocols, will provide authentication.

Non-Repudiation

Preventing a party from denying previous actions or commitments is known as the non-repudiation problem. The digital signature can be used to verify the identity of participants in a transaction and later enforce non-repudiation. A casino will need the services of non-repudiation if it is to enforce payment by players that have wagered and lost. In the next section, we generally define symmetric and public-key methods, their relative strengths, and weaknesses.

Cryptographic Background Art

This section lists five patents that provide the foundational art for public-key cryptography.

Patent number 5,231,668, the Digital Signature Algorithm (DSA). The DSA patent discusses signature schemes in a public-key context.

Patent 4,200,770, the Diffie-Hellman. The Diffie-Hellman patent is an important public-key patent and the described methods are often used for exchanging keys privately over a public network.

Patent 4,405,829, the RSA patent. The RSA patent describes the de-facto standard for public-key encryption around the world.

Patent 4,995,082, the Schnoor identification scheme. Schnoor developed an identification scheme that was later improved by the DSA patent. This patent then becomes prior art for the DSA patent.

The Alcorn 086 patent describes a public key authentication program for verification of the contents a hard disk and therefore a stored game. Authentication and encryption programs are not used for the confidentiality and

integrity of the digital information that is transferred back and forth between gaming machines, such as a slot machine and a casino server. As such, the present patent describes new art.

Public and Private Keys

Symmetric Key Cryptography

Symmetric-key cryptography, also known as secret-key cryptography, uses a unique key to exchange information between two parties. Therefore, the sender and the recipient of a message must share a secret, namely the key k. A well-known secret-key cryptography algorithm is the Data Encryption Standard (DES), which is used by financial institutions in a variety of capacities, including to encrypt PINs (personal identification numbers).

Given a message m, symmetric encryption function E, and key k, we will denote the encryption of m by E under k as $c = E_k(m)$ where c represents the ciphertext associated with message m. In order to decrypt c, we apply the decryption transformation $m = E_k^{-1}(c)$.

The preferred embodiment for symmetric key cryptographic functions is to use either one of the variants of DES such as DES, triple-DES, or DES-X or the forthcoming AES (Advanced Encryption Standard).

Claim

The use of a symmetric cryptographic algorithm, such as DES, or triple-DES to enforce privacy or authentication of information traveling in an information channel between gaming devices or a gaming server and a game.

Asymmetric-Key Cryptography

Asymmetric-key cryptography, or public-key cryptography, by contrast uses two different keys in a transaction. The asymmetric key pair consists of a public and private-key. The two keys are mathematically related so that data encrypted with either key can only be decrypted using the other. The public-key is made available to the world, while the private-key is kept secret. Entities desiring to send information to a particular individual will obtain the individual's public-key and encrypt information with that key. Only the holder of the private-key can then decrypt the information. This assurance is dependent upon not disclosing the private-key to anyone else. The essential feature of a public-key cryptosystem is that *knowledge of a public-key does not provide any computational information about the private-key.* One well-known public-key cryptography algorithm is RSA (named after its inventors Rivest, Shamir, and Adleman).

If we suppose that we have an asymmetric key pair (u,r), where u represents the public key component and r is the private key of the pair. Encryption and decryption of a message can be represented analogous to the symmetric case as $m = E_r^{-1}(E_u(m))$, where E_u represents the public encryption transformation and E_r^{-1} is the private decryption transformation. Unlike the symmetric case where there is one key, asymmetric cryptography uses a public key for encryption and the private key for decryption. We can use a public key cryptographic algorithm to create a digital signature.

The preferred embodiment for an asymmetric algorithm is either RSA or ElGamal.

Claim

The use of an asymmetric cryptographic algorithm, such as RSA, to enforce privacy or authentication of information traveling in an information channel between gaming devices or a gaming server and a game.

Public-Key Cryptographic Primitives

Suppose we have a large integer m, which may or may not be prime. Many important cryptographic algorithms require multiple precision arithmetic operations modulo m. Such arithmetic operations are said to take place in Z_m.

Some of the most important public-key cryptographic algorithms including RSA, Rabin, and ElGamal require efficient multiplication and exponentiation in Z_m. Exponentiation in Z_m is typically based on the more primitive operations of multiplication and addition in Z_m. Consequently, if we have a collection of algorithms that compute efficient arithmetic operations in Z_m, such as addition, subtraction, multiplication, squaring., and division, then we can build more complicated algorithms, such as exponentiation, greatest common divisors, and the Chinese remainder theorem. These in turn support RSA and other public key cryptographic algorithms.

The preferred embodiment for these mathematical cryptographic primitives is that they be implemented in hardware due to the computational complexity of the cryptographic algorithms that will utilize them.

Claim

The use of algorithms in a gaming machine or gaming server to perform arithmetic algorithms such as addition, subtraction, multiplication, squaring., and

division in Z_m, that is the integers modulo a large integer m. The integers that are operated upon by the algorithms are generally multiple precision and require special techniques for solution. These algorithms form the basis for public key cryptography.

Digital Signatures

By using public-key cryptography we can develop a class of a digital signatures. Suppose we have an asymmetric key pair (u,r) associated with E_u, the public encryption transformation and E_r^{-1}, the private decryption transformation respectively. A digital signature can be constructed by using the private encryption function to encrypt a message and allowing the receiver to verify the contents of the message by applying the public encryption function. The purpose of any digital signature is to help resolve disputes in a transaction. We will see that a trusted third party (TTP) will use a digital signature to promote trust in a public key that is being used to communicate on a network. In general, by a digital signature we mean any algorithm that has goals similar to that of the Digital Signature Algorithm (DSA), patent number 5,231,668.

A digital signature is one of the most important services provided by a certificate authority. The certificate authority will utilize a private signature algorithm, T_s and a private verification algorithm, T_v in order to prevent an active adversary from succeeding in impersonation on the network.

Claim

The use of digital signature algorithms, such as DSA, to ensure the authenticity of messages traveling in an information channel between gaming devices or a gaming server and a game.

Key Transport

While asymmetric cryptographic methods provide for efficient digital signatures, symmetric methods provide for more efficient encryption. Consequently, when sending a large message across a communication channel both symmetric and asymmetric methods may be employed. First a session key may be established using the asymmetric cryptography and then the message will be sent

The preferred embodiment for a key transport mechanism in a gaming environment is the X.509 strong two-way or three-way authentication mechanism.

Claim

The use of a hybrid encryption scheme that uses an asymmetric algorithm such as RSA for a session key exchange and a symmetric algorithm for message encryption.

The Gaming Environment

Suppose we have n gaming machines, g_1 through g_n, and a unique machine known as the gaming server that we will denote G. This configuration of one

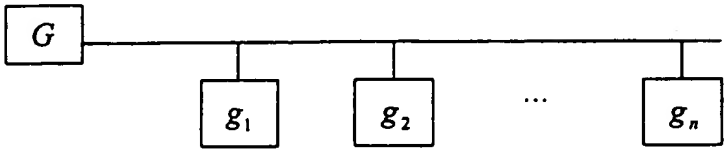


Figure 1. A model for the gaming environment.

server connected to many gaming machines can actually be a subsystem within a larger collection of gaming systems. Such a system may be connected to the Internet, or a WAN on which many such systems reside. The gaming server

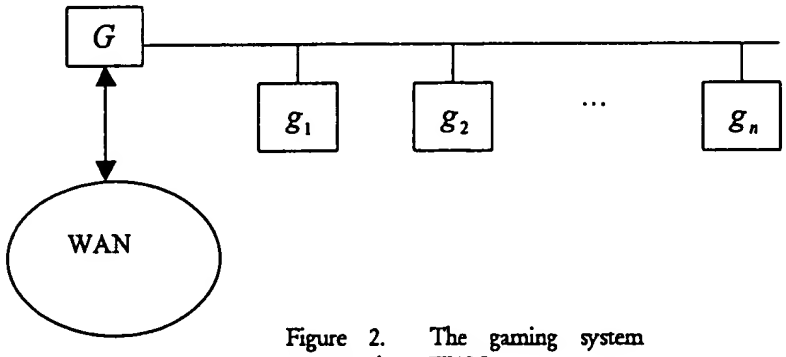


Figure 2. The gaming system connected to a WAN.

may have special equipment attached to it such as a router in order to facilitate the connection of the gaming machines it serves to the wider network. The computational capabilities of the server will generally exceed those of the gaming machines, at least with respect to cryptographic operations.

In addition to a WAN, each game g_i can service a set of players p_i. There may

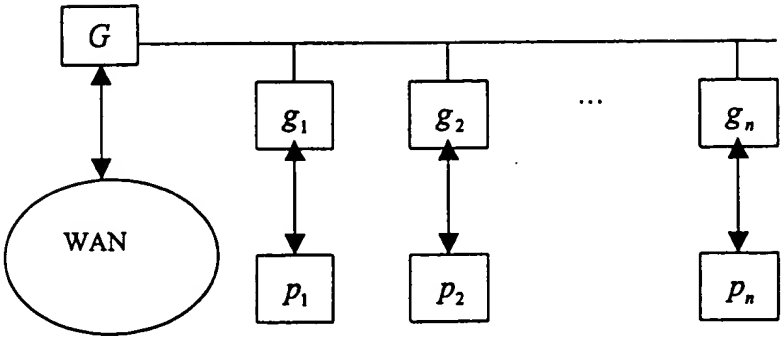


Figure 3. The gaming system with players at each game.

be more than one player in each p_i. Although the gaming server G can connect directly to a WAN, it will also be possible for each game g_i to connect to their own, possibly different, WAN. Such a combination allows the possibility for

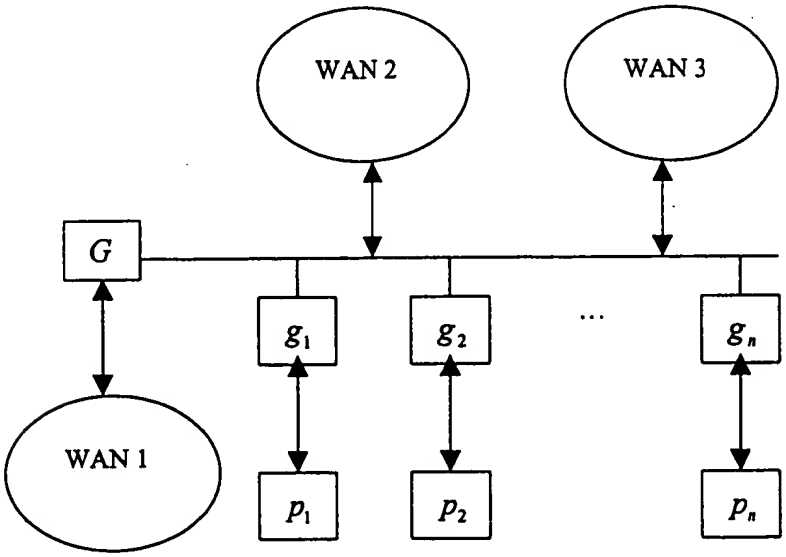


Figure 4. The gaming system with games having direct access to other networks, such as the Internet.

each gaming system within a casino to contain a WWW (World Wide Web) server in which not only local players can participate within a casino, but the same machine can service remote customers on a network. Such a system would allow local players to compete against remote players.

Motivation for a Trusted Third Party

The number of keys that must be stored locally has implications for both local storage and the complexity of key-update as machines are moved on and off the gaming network. Consider a network, as in figure 5, with five game machines each pair of machines requiring a private communication channel. A naieve

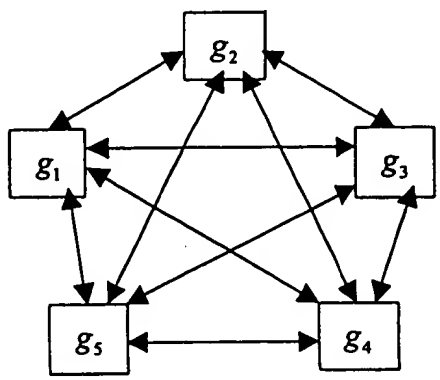


Figure 5. All pair keying without a TTP

symmetric key encryption system without a TTP will require up to 5 keys at each machine in order to facilitate the all pair communication problem. When one of the machines is moved off the network, all four other machines must ammend their key list by removing the now useless key. If a new machine is moved on the network then all five machines must ammend their key list by adding the new key. If one machine is compromised then the security of all the keys could be in question in which case all machines on the network must receive new keys. This last problem is known as the *key update problem* and is one of the primary motivations for public key cryptography. On a large network, key management

issues can be cost prohibitive unless they are given proper attention. If we are using symmetric key techniques then the solution is to use a TTP that maintains a list of all secret keys on the network and then issues session keys in order for two entities to communicate.

Symmetric Key Management

Consider the gaming system of figure 6. In this section we make the assumption that our Gaming Server G is trusted by all of the gaming devices g_1 through

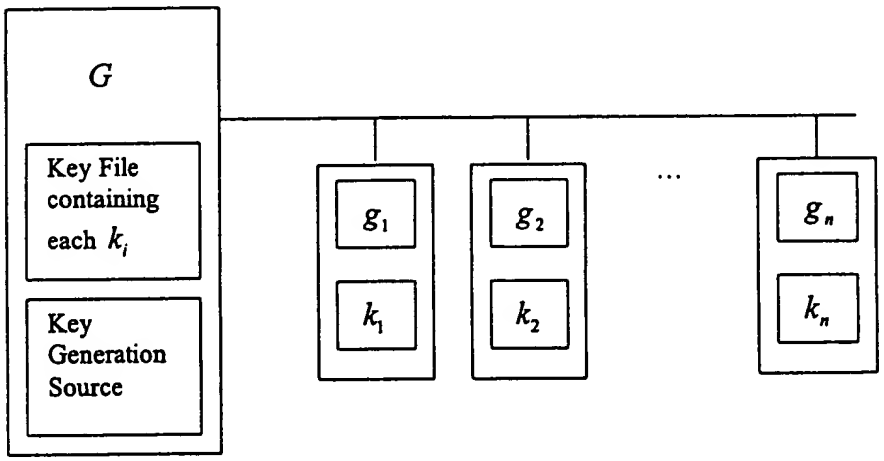


Figure 6. A gaming environment with a game server containing a key file and key generation source

g_n as a TTP. Each g_i shares a unique symmetric key, k_i with the TTP G. In the event that G and g_i need to communicate they can do so by encrypting their message using k_i. Assuming an adversary has access only to the communications channel and as long as the k_i is not compromised, the communication will be secure between G and g_i. If it is the case that an adversary can tamper with g_i then the k_i must be assumed to be insecure and therefore all communicatoin is insecure. Consequently we assume that physical

security is provided throughout the gaming environment so that such tampering cannot occur and each k_i is kept physically safe.

Suppose that we now would like to enable machine g_i to communicate securely with machine g_j. Server G contains a symmetric encryption function, E, such as DES or triple-DES that allows the encryption of a *session key*, k, that will be sent by G in an encrypted format to g_i and g_j. Let us denote that $E_{k_i}(m)$ represents the encryption of message m under encryption algorithm E using key k_i while $E_{k_i}^{-1}(m)$ represents the decryption of message m under encryption algorithm E using key k_i. In order to facilitate the session between g_i and g_j, G generates a new unique session key k and sends $E_{k_i}(k)$ to g_i and $E_{kj}(k)$ to g_j. Machines g_i and g_j can now communicate securely because they can each recover k by forming $k = E_{k_i}^{-1}(E_{k_i}(k)) = E_{k_{jl}}^{-1}(E_{k_j}(k))$. Using the session key k, If g_i wants to communicate message m to machine g_j then g_i sends $E_k(m)$ to g_j and g_j forms $m = E_k^{-1}(E_k(m))$ to recover the message.

Although it is easy to add and remove machines from a gaming network using this scheme, the server G needs a copy of all the keys and if the server is compromised then all communication on the network is compromised. An advantage for each g_i is that g_i must store only one long term key but a disadvantage is that inter-machine communication takes place using a generated session key. Such a procedure consumes extra time and bandwidth since the server needs to provide the session key for each period of communication for which the session key is valid. Although it was mentioned that communication between a gaming machine and a server can take place using the shared secret key of the gaming machine, in practice a session key will be generated by the

server as with inter-machine communication in order to protect the long-term secret key of the gaming machine. Eventually we will see that players on the network will require services of confidentiality and non-repudiation that are better facilitated by public-key cryptographic mechanisms.

Claims

1. A computer acting as a symmetric key server for the network of game machines that maintains the list of long term symmetric keys for the network.

2. A computer acting as a symmetric key server that generates session keys based on the long term symmetric keys and a random number generator (rng). The term random number generator and associated abbreviation rng will represent either pseudo-random number generator or random number generator without loss of generality since either will be a source of random numbers that has been approved by the regulatory establishment. Each of the long-term keys held by the symmetric key server corresponds to one of the keys held by the individual gaming machines on the network.

3. A computer acting as a symmetric key server that encrypts a session key with the long-term symmetric key of a particular machine and then transmits the encrypted session key to that particular machine. In doing so for several machines on the network, each machine can decrypt the particular message sent and retrieve the session key which can then be used to encrypt session messages on the network.

4. The session key may have a time stamp associated with it that causes the key to be valid for a specified period of time.

Asymmetric Key Management

Suppose that instead of each gaming machine keeping a symmetric key, that it keeps the private key of an asymmetric pair. When two machines need to pass a message, they request the public key of the intended receiver, encrypt the message with the public key of the receiver and then send the message to the

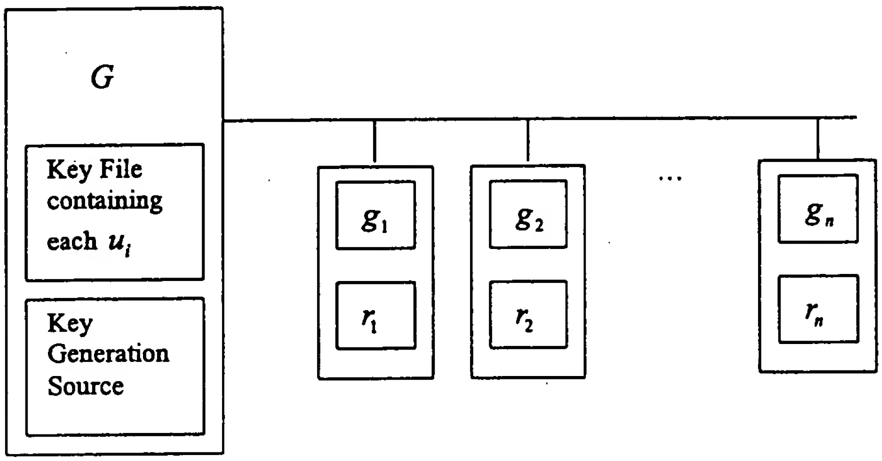


Figure 7. A gaming environment with public and private keys.

receiver. This procedure may be just one step in a more elaborate protocol. The receiving machine decrypts the message using the private key to that machine.

An advantage of the asymmetric key approach is that the server G no longer needs to be a TTP, unlike the asymmetric approach to key management. In fact, the public key file could reside anywhere on the network so long as it was accessible by all network members that needed to communicate. Another advantage is that there are only n keys to manage. Communication between entities on the network can proceed securely provided that there are only passive adversaries on the network.

If there is an active adversary that manages to alter the public-key file then the adversary can impersonate anyone on the network for which there is a falsified

key in the public key file. Prevention of such an attack can be accomplished by the use of a TTP to certify the owner of a particular public key. Such a TTP is known as a certificate authority and the combination of the signed key along with the signature is the basis for what is known as a digital certificate.

Claims

1. A computer acting as an asymmetric key server for the network of game machines that maintains the list of public keys for the network. The key server will send the public component of an asymmetric key upon request to a receiver on the network.

2. A computer acting as an asymmetric key generator for the network of gaming machines that generates asymmetric keys based on a random number generator (rng) and a key generator algorithm that produces public-private-key pairs suitable for use in asymmetric cryptographic algorithms such as RSA.

Certificate Authorities and Public-Key Management for Gaming

Cryptographic services are able to fullfill their intended purpose to the extent that the keys used by the services are secure. If there is any doubt about the security or associated identity of a particular key, then the key must be replaced with a fresh key that can be trusted. The key becomes the secret in any transaction on an open network. Such transactions include message passing between gaming machines as well as secure data storage using public key mechanisms. We have seen that if there is a public key file and no means for guaranteeing the integrity of the public keys in the file, then this leaves the possibility for an active adversary to replace keys in the file and impersonate members of the network. In a gaming environment, this could lead to an

adversary impersonating the house and accepting electronic payments from games and players in the casino.

There are symmetric-key certificate authorities, but we will not consider them in this document. The term certificate authority, or CA, will be used to mean public-key certificate authority. A primary role of the CA is to guarantee that identity of an entity granted a unique certificate. The certificate represents a verifiable binding of a public key to that entity. Usually, the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because the CA can be used to guarantee the identity of two parties exchanging information.

Certificates

A certificate consists of a signature part and a data part. Consider figure 8.

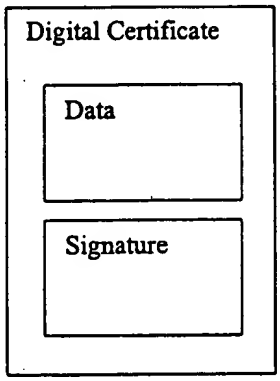


Figure 8. A Digital Certificate

This certificate authenticates the identity of the owner of the public key to the extent that the digital signature is secure and the TTP is actually trusted.

Information contained in the data part consists of the public key of the entity along with other information such as:

1. name or mailing address for the individual associated with the certificate
2. serial number and validity period for the public key
3. use parameters and algorithms for the public key
4. verification details for the public key such as the CA name and algorithms

The signature portion of the certificate consists of the CA's signature over the data part. If an individual wishing to use a particular public key finds that the signature in the associated certificate does not verify then they know not to use the associated public key.

The CA uses a private signing function T_s to create the signature over the data portion for the certificate. The CA publishes a public verification algorithm T_v that others can use to validate certificates issued by the CA. The algorithms T_s and T_v are often based on public key digital signatures.

Creation of Certificates

Prior to issuing a certificate for an entity, such as a gaming machine or player at a casino, the CA must have proof of the identity of the entity. Such proof can often take the form of a passport, driver's license, or other approved legal document. In the case of a machine, the regulatory agency might generate an asymmetric key pair and sign the public key. Once the regulatory agency signature is verified it is possible to generate a certificate at the casino and install the machine. In the case where there is perhaps more than one certificate authority, we now have multiple domains of trust to consider. Establishing trust across multiple domains will be the subject of the next section.

The preferred embodiment for a certification authority for gaming is in accordance with the X.509 (ISO/IEC 9594-8) standard.

Claims

1. A gaming server acting as a CA with a private signing function that is used to create certificates.

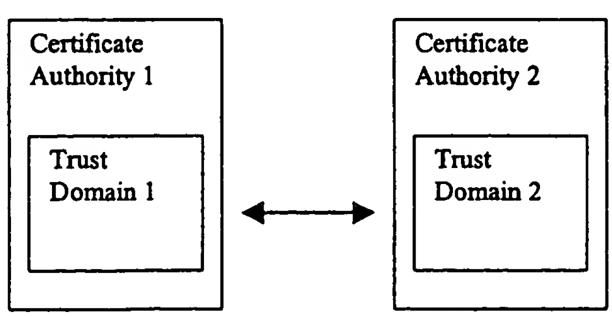
2. A gaming server acting as a CA that publishes a corresponding public verification function so members of the trust domain under the CA can verify the contents of the certificate and validate the authenticity of a public key.

3. A gaming server acting as a CA that maintains a revocation list of certificates that are no longer valid.

4. A gaming server acting as a CA that generates asymmetric key pairs. The CA does not always generate such key pairs because it places complete trust in one entity.

Multiple Domains of Trust

In a given gaming jurisdiction there could be many certificate authorities, each establishing trust in their respective domains. For example, each casino could establish a certificate authority and manage the CA over the games in the casino. A regional regulatory authority might provide a single point of trust over all



casinos in its jurisdiction. A company that manages several casinos might have a hierarchical set of certificate authorities, each CA managing trust at a casino, with the root CA managing trust over the collection of casinos. To solve the trust issue across several gaming and trust domains we propose a hierarchical trust model for gaming CAs. The general use of a CA also admits other trust models, such as the more general digraph trust model or the multiple rooted trees model, but we will consider the use of the strictly hierarchical model in this patent as the preferred implementation. In figure 10 we have a collection of CAs with the root CA directing trust along the directed edges eventually to the leaves, consisting of participants and gaming machines, that use the hierarchy of CAs to establish a trusted relationship amongst themselves. Such a mechanism might allow for dynamic relationships between games at geographically different casino

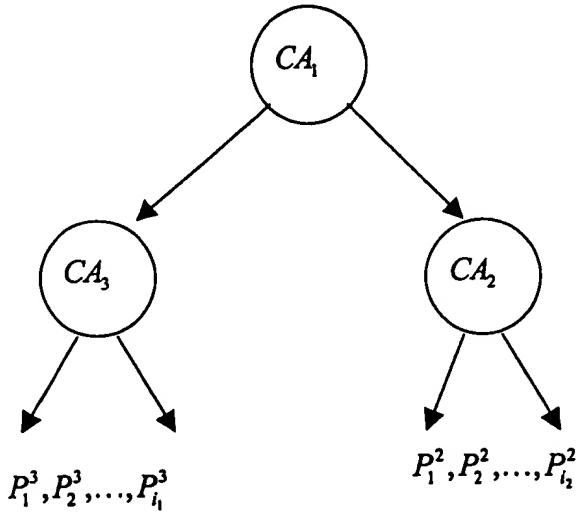


Figure 10. A hierarchical trust model for certificate authorities

locations or under different casino ownership.

Consider for example the case where the holder of a public key, P_1^3 in the trust domain controlled by CA_3 needs to communicate with an entity P_1^2 in the trust domain of CA_2. The holder of P_1^3 needs to validate the certificate of P_1^2 in order

to develop trust in the public key of P_1^2. Let $CA_1\{CA_2\}$ represent the certificate signed by CA_1 binding the name CA_2 to P^2, the public key for CA_2. Given initial trust in P^1, the public key of the root CA, the holder of P_1^3 can use the public verification algorithm of CA_2 to extract a trusted copy of P^2 from the certificate chain $\{CA_1\{CA_2\}\}$. The public key P^2 can now be used to validate the authenticity of the certificate containing P_1^2.

Claims

5. A gaming server acting as a CA with a private signing function that is used to create certificates for other CAs.

Extending the gaming network beyond the physical boundary of the Casino

Here we leverage our public key infrastructure to extend the gaming network beyond the casino. A device for a direct Internet connection to a slot machine, or a server that interfaces in real-time to a particular slot machine. Such a connection would allow an outside user to play a particular machine from anywhere there is a network connection, possibly anywhere in the world. Extending the availability of gaming machines beyond the boundaries of in individual casino gives the casino the ability to grow their market virtually and leverage their existing investment in games.

In order to give the player more control in the case where a game is simultaneously being used by a local casino participant and a on the network, we introduce a new device, the *Internet Access Switch* (IAC).

The Internet Access Switch

This device can be attached to the slot machine so that an Internet connection can be disconnected while a user is playing. This gives the player the advantage of knowing his play will not be interrupted or tampered with from a potential player on the Internet. It gives the player an added measure of control. There is an auto-return on the switch to reconnect the system after a certain period of non-play at the machine. The auto-return feature hooks up the machine after a certain period back to the Internet to return the machine to use so that on-line participants can again use it. The lockout works the other way as well. If an Internet player is using the machine then the lockout feature will not allow a user on the floor to play the slot. Of course, a machine can be designed as a server so that both on-line and on-site players can both theoretically play a given machine at the same time. This exclusivity gives the players a sense that the machine belongs to them during their cycle of play and therefore that they are in control.

Notation

E - Encryption algorithm

E^{-1} - Decryption algorithm of E

g_i - Gaming machine i.

p_i - Player i.

k_i - Key i

S - The gaming server

u_i - The public component of asymmetric key pair i.

r_i - The private component of asymmetric key pair i

c - Cyphertext

$CA_1\{CA_2\}$ - represent the certificate signed by CA_1 binding the name CA_2 to a public key.

m - Message

TTP – Trusted Third Party

CA – Certificate Authority, a TTP in the public key case

T_s - private signing function used by a TTP

T_v - public verification algorithm used by a TTP